

## UNITED STATES DISTRICT COURT

FILED

WESTERN

for the  
DISTRICT OFOKLAHOMA APR 30 2019

In the Matter of the Search of  
(Briefly describe the property to be search  
Or identify the person by name and address)

## PROPERTY KNOWN AS:

Black Alcatel One Touch Cellular Phone,  
Model #A570BL, Build: vE9G-UTG0

## IN THE POSSESSION OF:

Federal Bureau of Investigation  
3301 W. Memorial Road  
Oklahoma City, OK 73134

CARMELITA REEDER SHIN  
CLERK, U.S. DISTRICT COURT  
BY: DEPUTY

Case No. M-19-215-SMAPPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following [Person or Property?] (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2252A(a)(5)(B)

Offense Description

Possession of child pornography.

The application is based on these facts:

See attached Affidavit of Special Agent Kristina D. Chen, Federal Bureau of Investigation, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of \_\_\_\_\_ days (*give exact ending date if more than 30 days*) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

  
Applicant's signature

KRISTINA D. CHEN  
Special Agent  
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: 4-30-19

City and State: Oklahoma City, Oklahoma

  
\_\_\_\_\_  
*Judge's signature*

SUZANNE MITCHELL, U.S. Magistrate Judge  
*Printed name and title*

**AFFIDAVIT**

I, Special Agent Kristina D. Chen, being duly sworn, depose and state the following:

**I. INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation and have been since July 7, 2018, and I am currently assigned to the FBI Field Office located in Oklahoma City, Oklahoma. As an FBI Special Agent, I conduct investigations relating to federal criminal violations, to include child exploitation. I have been involved in executing arrest warrants of such offenders. Through my training and experience, I have gained knowledge related to conducting this type of investigation. I have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 2252A(a)(5)(B), and I am authorized by the Attorney General to request a search warrant.

2. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of a violation of 18 U.S.C. 2252A(a)(5)(B) (possession of materials containing child pornography) are located in an electronically stored data device, to wit: black Alcatel One Touch Cellular Phone, model # A570BL, Build: vE9G-UTG0, which is currently in the custody of the FBI in Oklahoma City and more particularly described in Attachment A (hereinafter the "SUSPECTED DEVICE"). I submit this application and affidavit in support of a search warrant authorizing a search of the entire SUSPECTED DEVICE for evidence, fruits and instrumentalities of the foregoing criminal violation more fully described in Attachment B and to seize all items listed in Attachment B.

3. The information contained in this affidavit is based on my training, experience, and participation in other investigations. The current investigation has involved discussions between law enforcement officers, interviews of witnesses, review of documents and computer records, and communications with others who have personal knowledge of the events and circumstances described herein. Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, it does not set forth every fact that I or others have learned during this investigation.

## **II. COMPUTER TERMS AND GENERAL DEFINITIONS**

4. The term “child pornography” as used herein is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

5. “Cellular phone” is a portable telephone that can make and receive calls using a communication network known as a cellular network. Cellular phones support a variety of other services, such as text messaging, Multimedia Messaging Service (MMS) (a standard way to send messages that include multimedia content to and from a mobile phone over a cellular network), email, Internet access, video games, and digital photography.

6. “Computer,” as used broadly herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or

operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

### **III. BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE**

7. On 06/26/2018, Special Agent Kevin B. Hall, Jr., was contacted by Lieutenant (LT) Tony Krebs, Choctaw Nation Tribal Police (CNTP). LT. Krebs reported having custody of a cell phone that contained an image of child pornography.

8. The phone, later identified as the SUSPECTED DEVICE, was located by the Choctaw Nation Tribal Security (CNTS) on or about 06/20/2018, after it was left unattended in one of the buffet areas of the Choctaw Casino and Resort (CCR), 4216 U.S. 69, Durant, Oklahoma, 74701. Upon picking up the SUSPECTED DEVICE, CNTS noticed an image of a young naked female with her legs spread open displayed as the phone's wall paper. The young naked female appeared to be posed provocatively, exposing her nude vagina to the camera. The CNTS believed the image to be child pornography and looked through the SUSPECTED DEVICES' files to locate the owner. The owner was identified as Danny Lynn Love.

9. On or about 06/20/2018, Love went to the casino staff to report a lost phone. Upon being notified that Love was looking for a lost phone, a CNTS officer spoke to Love who stated he lost the phone five (5) months ago. However, Love acknowledged the SUSPECTED DEVICE was the lost phone. On or about 06/20/2018, CNTS spoke to Sara Spiegel, the girlfriend of Love. Spiegel stated she found the SUSPECTED DEVICE in the home of Love. Spiegel brought the SUSPECTED DEVICE to the CCR. While in the CCR, Spiegel lost control of the phone in or around the area of the Butterfield's Restaurant.

10. On or about 07/11/2018, Special Agent Kevin B. Hall, Jr., received the SUSPECTED DEVICE from LT. Krebs after LT. Krebs requested the investigative assistance of the FBI.

The SUSPECTED DEVICE was placed into evidence and stored in the FBI - Oklahoma City Field Office, 3301 W. Memorial Road, Oklahoma City, Oklahoma 73134, where it has remained pending the granting of legal authority and forensic examination.

#### **IV. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

11. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

12. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken, it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store more than 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

13. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has

drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

14. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Also, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

15. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

16. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-

mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

17. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

18. Often computers and hand-held computing devices provide location information as to a computers specific location when it was used. This evidence is valuable in tracking past locations of the computer and often the user and owner of said computer.


19. Digital files such as movies and pictures can be quickly and easily transferred back and forth between devices or stored simultaneously and indefinitely on both devices. Such devices, even very small ones, can store very large amounts of digital files.

## **V. CONCLUSION**

20. Based on the foregoing, I believe there is probable cause that a violation of 18 U.S.C. § 2252A(a)(5)(B) has been committed and that evidence, fruits, and instrumentalities of the offense, more fully described in Attachment B, will be found by searching the SUSPECTED



DEVICE, located at FBI, Oklahoma City Field Office, 3301 W. Memorial Road, Oklahoma City, Oklahoma, 73134. I respectfully request that this Court issue a search warrant for the SUSPECTED DEVICE more fully described in Attachment A authorizing the seizure and search of the items described in Attachment B.

  
\_\_\_\_\_  
Kristina D. Chen  
Special Agent  
Federal Bureau of Investigation

Sworn to me this 30 day of April, 2019.

  
\_\_\_\_\_  
Suzanne Mitchell  
United States Magistrate Judge

**ATTACHMENT A**

***Items to be Searched***

The following items are currently being held as evidence in the custody of the Federal Bureau of Investigation (FBI) Oklahoma City Field Office, 3301 W. Memorial Road, Oklahoma City, Oklahoma, 73134:

1. Items released to the FBI from the Choctaw Nation Tribal Security:
  - a. Black Alcatel One Touch Cellular Phone, model # A570BL, Build: vE9G-UTG0
  - b. The device appears to be a smart phone

**ATTACHMENT B**

***Evidence to be Seized***

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely, a violation of Title 18, United States Code, Section 2252A(a)(5)(B):

For any cell phone or storage medium whose seizure is otherwise authorized by this warrant, and any cell phone or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "SUSPECTED DEVICE"):

- a. evidence of who used, owned, or controlled the SUSPECTED DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the SUSPECTED DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the cell phone was accessed or used to determine the chronological context of cell phone access, use, and events relating to crime under investigation and to the cell phone user;
- e. evidence indicating the cell phone user's state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the SUSPECTED DEVICE of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUSPECTED DEVICE;
- h. evidence of the times the SUSPECTED DEVICE was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the SUSPECTED DEVICE;
- j. documentation and manuals that may be necessary to access the SUSPECTED DEVICE or to conduct a forensic examination of the SUSPECTED DEVICE;
- k. records of or information about Internet Protocol addresses used by the SUSPECTED DEVICE;
- l. records of or information about the SUSPECTED DEVICE Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.
- n. Routers, modems, and network equipment used to connect computers to the Internet.
- o. Child pornography and child erotica.
- p. Records, information, and items relating to violations of the statutes described above including: cords and information relating to the identity or location of the persons suspected

of violating the statutes described above; and as used above, the terms “records” and “information” includes all forms of creation or storage, including any form of cell phone or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "storage medium" includes any physical object upon which cell phone data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.